



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/072,260	02/06/2002	James D. Pravetz	07844-497001	3277

21876 7590 03/22/2006

FISH & RICHARDSON P.C.
P.O. Box 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER

SZYMANSKI, THOMAS M

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 03/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<p align="center">Office Action Summary</p>	Application No. 10/072,260	Applicant(s) PRAVETZ, JAMES D.	
	Examiner Thomas Szymanski	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 13 December 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-49 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-49 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|--|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
6) <input type="checkbox"/> Other: _____ |
|--|--|

DETAILED ACTION

1. Claims 1-49 have been examined.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-7, 9-10, 12-17, 19, 21-28, 30-36, 38-39, 41-46, and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier as applied to claim 1, and further in view of Stallings.
4. Schneier teaches a system for the communication of secure electronic mail using certificates. Schneier fails to teach explicitly requesting the recipient's certificate within the initial message.
5. However, Stallings teaches authentication between two users (pg 451 figure 14.6) within which certificates are used to verify the identity of each party and the certificates are presented and requested within the initial message denoted by Stallings as a phase.
6. It is desirable within any secured communication system to be able to expeditiously authenticate between the two parties involved. Stallings teaches this method of quick reliable authentication using the SSL handshake protocol, by providing the server's certificate with the initial request for the clients certificate so as to provide

for fewer communications between the two parties, as such decreasing the time spent on authenticating and increasing the security by initially being authenticated instead of waiting for several other messages to be exchanged.

7. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the schema for authentication of parties under Stallings into the privacy enhanced mail system described by Schneier for the advantages of increased security and increased speed of communications.

8. Regarding Claim 1: Generate a first container object with a recognizable container type which is associated with an application (Schneier Fig 24.4-5) As shown an electronic message comprises the means for containing all necessary information related to the message. The container type is the email message format associated with the email application being used.

Containing a sender's certificate or request (Schneier Fig 24.5, Stallings Fig 14.6) As denoted the message contains the sender's certificate and additionally any necessary issuer's certificates.

Containing a request for a recipient's certificate (Stallings Fig 14.6) Within the figure as shown by Stallings the container herein described as the message is composed of the sender's certificate, a certificate request, and other necessary information. In this way the message provides for requesting the certificate of the recipient.

Container has a recognizable type (Schneier pg 577-578, Fig 24.4-5 , Stallings Fig 14.6) As described the message has a recognizable type of an electronic mail message, and

additionally provides for identification of the separate encryption protocols that may be used in forming the message.

Transmit container to recipient's address (Schneier pg 577, 581 lines 12-18) As the message is described of being an email it is understood that an address of such a recipient is provided and logically transmitted thereto.

Receive a second container object having the same type as the first; automatically identify and extract one or more certificates (Stallings fig 14.6) Within the combined system it is inherent for the determination of certificates to be automatic as inherently provided by Stallings.

9. Regarding Claim 2: Receive input from sender specifying recipient's address (Schneier pg 579, Fig 24.4-5) As within any typical email message the user must provide for the destination or recipient with which the communication is desired. Specifying one or more certificates of the sender (Schneier pg 577, 24.5) The message may contain one or more certificates of the sender depending on the nature of the certificate. If the certificate is issued by the sender itself, meaning the sender is a certificate authority (CA), then only that one certificate would be present. In the event the sender is not a CA then the issuer certificate would be available with the sender's certificate.

10. Regarding Claims 3, 10, 15 and 19: transmitting/receiving the container by electronic mail (Schneier pg 577 lines 29-34) As described by Schneier the system provides electronic mail over the internet.

Transmitting/receiving by HTTP (Schneier pg 577 lines 29-34) As stated above the system provides for electronic mail over the internet. As it is known electronic mail is not confined to a single method but is provided for in many ways. Electronic mail is available over the internet via web-based email services such as Yahoo.com for example. In such an exemplary situation the container or message is communicated over HTTP to the end user for viewing, as such providing for transmission by HTTP.

Transmitted/Received via a networked server (Schneier pg 577 lines 29-34) Any communications that take place via a network such as those stated herein occur through a networked server and as such information is received and sent through such means.

11. Regarding Claim 4: First container object generated by a server (Schneier pg 577 lines 29-34, Fig 24.5) The message is generated within the computer medium of either the sender's system or the server of the HTTP based web-mail system. In either instant case the computer within which the message is created is a server. In the case of the web-mail system the machine is a server of that email system allowing for those mail functions. In the case of the sender's system the computer acts as a server for basic functions such as the mail functionality of the system. A server is defined as the software component of one device that provides services for use by clients on the same or another device.

12. Regarding Claims 5, and 16: Receive input selecting one or more of the multiple certificates (Schneier Fig 24.5, pg 579-582) The system of the sender provides the input

based on the nature of the sender's certificate, as stated above if the issuer is different than the originator (sender) then multiple certificates may be selected.

Retrieve the selected certificates from a database (Schneier pg 579-582) As stated on page 579 lines 1-18 the certificates are certified by Certificate Authorities, which contain such certificates within databases. In order to provide the certificates the CA must retrieve those necessary certificates from a database.

Include the selected certificates in the container object (Schneier Fig 24.5, Stallings Fig 14.6) As noted the certificates are incorporated into the container (message).

13. Regarding Claim 6: receive input from sender specifying a return address (Schneier pg 577 lines 28-34) The functionality of an electronic mail system requires the sender's address to be incorporated into the outgoing message

Instructions for returning recipient's certificate (Stallings Fig 14.6, Schneier Fig 24.4-5) The instructions for returning the certificate are simply the request itself and the return address as provided.

Include address and instructions in the first container object (Stallings Fig 14.6, Schneier Fig 24.4-5) As shown these items are included in the message as necessary functional pieces.

14. Regarding Claims 7, 17, and 22: object validation information to be used to validate the certificate (Stallings pg 454-455, Schneier Fig 24.4-5, pg 579) Along with any provided certificate there must be validation information as is the functional structure of such an item to allow the client to authenticate such means. This is

provided generally by way of listing of the CA and specific identification of the certificate in reference to its issuer.

15. Regarding Claim 9: Receive a container from a second instance of the application having a recognizable type (Stallings fig 14.6, Schneier pg 578) As defined the message has a recognizable type of an electronic mail message, and additionally provides for identification of the separate encryption protocols that may be used in forming the message.

Recognize the container may include a certificate (Schneier Fig 24.5) The message as defined contains a certificate

Automatically determine if the container object contains a certificate of the sender (Stallings Fig 14.6, Schneier Fig 24.5) The logical process of validating the sender determines if a certificate is present as is automatically determined within the system of Stallings.

16. Regarding Claim 12: If certificate is valid, extract and store certificate (Schneier Fig 24.5, pg 579-581) The certificate if validated allows for reading of the message and decryption of the encrypted content and thus it is stored within the memory of the system. In the event a message does not authenticate it would not be retained since an invalid message serves no purpose but to waste resources of the system.

17. Regarding Claim 13: Automatically determine if the first container object has a request for a recipient's certificate (Schneier Fig 24.5, Stallings fig 14.6, pg 450-452)

Respond to request (Stallings fig 14.6, Schneier pg 577 lines 28-34) As shown in the figure a response is constructed as a second message (phase) with the certificate of the recipient.

18. Regarding Claims 14 and 21: Generate a second container including a certificate of the recipient (Stallings fig 14.6, Schneier pg 577 lines 28-34) As is noted the certificate is included in a reply to the sender's request

Extract a return address from the first container and transmit second container to that address (Schneier pg 577 lines 28-34) The structure of the message as outlined previously provides for a return address.

19. Claims 23-28, 30-36, 38-39, 41-46, 48 are a computer program product instruction and method implementation of claims 1-7, 9-10, 12-17, 19, and 21-22, and as such are rejected on the same basis.

20. Claims 8, 11, 18, 20, 29, 37, 40, 47, and 49 as best understood are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier and Stallings as applied to claim 1, and further in view of The PDF Reference, Second Edition.

21. Schneier and Stallings teach a system as in claim 1 for the exchange of certificates via electronic mail, but fail to teach the use of Forms Data Format.

22. The PDF Reference, Second Edition teaches the use of The Forms Data Format for submission and retrieval of information (pg 485 lines 1-26) via a server.

23. Separating out extra information from a message and forming it into a common file layout is a desirable feature since this process adds cross-platform compatibility and

the advantages of increased security by allowing further methods of protecting the given data and additionally adding further functionality through the ability to append such a file to any message format.

24. It would have been obvious to one skilled in the art at the time of the applicant's invention to combine the Forms Data Format of the PDF Reference, Second Edition with the system outlined by Schneier and Stallings. The added functionality and security features that are obtained from such a combination are desirable within any such system.

Response to Arguments

25. Applicant's arguments filed 12/13/2005 have been fully considered but they are not persuasive.

26. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

27. Regarding the applicant's argument of the combined reference not teaching automatically identifying and extracting one or more certificates, attention is directed to the Stallings reference, wherein Fig 14.6 and associated discussion (450-455), the explanation of such an implementation clearly delineates the nature of such a protocol being automated so as to automatically determine the presence of such objects and their manipulation as outlined.

28. As presented within the Stallings reference the process of determining if a certificate is present is an automated process dictated by the handshake protocol.

29. The execution of such a protocol is not mandated by a mental step, but rather by the application that implements such steps. In the instant case the protocol is implemented within an email system that inherently provides for automating such functionality.

30. Regarding the applicant's argument that Stallings does not teach the container object. The applicant's attention is directed to the piecemeal analysis argument provided above and further to the combined reference wherein Schneier teaches a container format.

31. Regarding the argument of Schneier not teaching automatically detecting a certificate attention is directed to the above statements of Stallings and the combined reference as such steps being inherent within the combination.

32. With respect to the applicant's arguments concerning additional claims: All arguments are believed to be addressed within the above statements.

Conclusion

33. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

34. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Applicant is reminded that in amending in response to a rejection of claims, the patentable novelty must be clearly shown in view of the state of art disclosed by the references cited and the objections made. Applicant must show how the amendments avoid such references and objections. See 37 CFR 1.111(c).

35. Inquiries concerning this communication or earlier communications from the examiner should be directed to Thomas M. Szymanski who can be reached at (571) 272-8574. The examiner's normal working schedule is between the hours 8:00am – 4:30pm (EST), Monday – Friday.

36. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached at (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

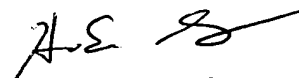
37. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for

Art Unit: 2134

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



HOSUK SONG
PRIMARY EXAMINER